

DEPARTMENT OF DEFENSE				1. CLEARANCE AND SAFEGUARDING	
CONTRACT SECURITY CLASSIFICATION SPECIFICATION				a. FACILITY CLEARANCE REQUIRED	
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				Secret	
b. LEVEL OF SAFEGUARDING REQUIRED				Secret	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
<input type="checkbox"/>	a. PRIME CONTRACT NUMBER		<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases) Date (YYMMDD)	
<input type="checkbox"/>	b. SUBCONTRACT NUMBER		<input type="checkbox"/>	b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER	Due Date (YYMMDD)	<input type="checkbox"/>	c. FINAL (Complete Item 5 in all cases) Date (YYMMDD)	
	FA8709-04-R-0002				
4. IS THIS A FOLLOW-ON CONTRACT?			NO. If Yes, complete the following:		
<input type="checkbox"/>	YES	<input checked="" type="checkbox"/>	(Preceding Contract Number) is transferred to this follow-on contract.		
Classified material received or generated under					
5. IS THIS A FINAL DD FORM 254?			NO. If Yes, complete the following:		
<input type="checkbox"/>	YES	<input checked="" type="checkbox"/>	In response to the contractor's request dated, retention of the classified material is authorized for the period		
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)		
TBD					
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)		
TBD					
8. ACTUAL PERFORMANCE					
a. LOCATION		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)		
TBD					
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
Pre-System Development and Demonstration for Airborne, Maritime, and Fixed Station JTRS					
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION				e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)		<input type="checkbox"/>	<input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI		<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	
g. SECRET INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify)	
				See Block 13 Notification of Government Security Activity Clause applies (May 96) ESC/NI, 5 Eglin St. Hanscom AFB, MA 01731-1620	

12. PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

☐ Direct

☒ Through (Specify)

ESC/PA

9 Eglin Street

Hanscom AFB, MA 01731-2118

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional names as needed to provide complete guidance.)

-Any classified information generated in the performance of this contract shall required contractor to apply derivative classification and markings consistent with source material or be governed by the JTRS Security Classification Guide. Which is currently in revision.

-The requirements, restrictions and the safeguards prescribed by the NISPOM, DoD 5220.22-M, dated January 1995 as well as any changes, modifications or revisions to this document and its supplements apply to all classified contract performance.

-Ref Block 10a and 11h - COMSEC. See attachment 1

-Ref Block 10e(2) - Non-SCI. See attachment 2

-Ref Block 10g - NATO. NATO Briefings are required for all personnel working/visiting the installation.

-Ref Block 10j. - FOUO. See attachment 3

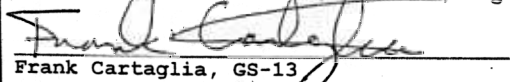
-Ref Block 11i - TEMPEST. See attachment 4

Ref Block 11k - DCS. DCS address is HQ Defense Courier Service Bldg P-830, Ft. George G. Meade, MD 20755-5370

-Contract Expiration:

-Program Manager: LtCol Maryann P. Watson, ESC/NI4, Bldg 1612, 5 Eglin Street, Hanscom AFB 10731

-Contract Monitor: Rick Fox, ESC/NI4K, Bldg 1612, Hanscom AFB, MA 01731


Frank Cartaglia, GS-13
Chief, Security NIO


Al Knoll, EMSEC Manager 3 Dec 03

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

☒ Yes ☐ No

OPSEC requirements apply to this contract. See Attachment #5

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

☐ Yes ☒ No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

Richard Fox

b. TITLE

PCO

c. TELEPHONE (Include Area Code)

478-6395

d. ADDRESS (Include Zip Code)

**ESC/NI4K
Bldg 1612
5 Eglin Street
Hanscom AFB, MA 01731**

17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY ESC/INP |

e. SIGNATURE

 12-3-03

ATTACHMENT 1

COMSEC

(Communications Security)

DD Form 254, Block 10a & 11h:

The National Security Agency Industrial COMSEC Manual (NSA Manual 90-1), shall apply to this contract. Access to classified COMSEC information shall be restricted to U. S. Citizens who: have been granted a final government security clearance; have a valid need-to-know (as defined in the National Industrial Security Program Operating Manual (NISPOM)); and have successfully completed a non-lifestyle, counterintelligence scope polygraph examination if required, administered in accordance with DoD or agency requirements and applicable laws. Non-U. S. Citizens, including immigrant aliens, are not eligible for access to classified COMSEC material or information. Access to unclassified, Controlled Cryptographic Items (CCI) will be limited to U. S. Citizens requiring such access. Within the U. S, Non-U.S. Citizens may perform building maintenance or custodial duties in contractor spaces containing installed CCI equipment, provided that equipment is not keyed. For access to certain types of COMSEC information, a CRYPTO access or COMSEC briefing may be required. Refer to Section II, Paragraph 9, of NSA Manual 90-1 for briefings required under specific types of access. The Facility Security Officer (FSO) must provide a current listing of all individuals granted cryptographic access for each contract or Memorandum of Agreement (MOA) to the appropriate government Program Office.

ATTACHMENT 2

DD Form 254, Block 10e(2) : Non-SCI

ADDENDUM FOR
GENERAL INTELLIGENCE MATERIAL/FOREIGN DISCLOSURE

1. Special Requirements for General and Foreign Intelligence Material. In addition to the requirements and controls for classified material, the Director, Central Intelligence, sets up additional requirements and controls for intelligence in the possession of contractors. The contractor must:

a. Maintain control of all intelligence materials released in his or her custody in accordance with DOD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM), January 1995, paragraphs 5-200, 201 and 202 for control. Contractors agree that all intelligence material released, all reproductions and other material generated (including reproductions) are the property of the US Government.

b. Maintain control of all reproduced intelligence data in the same manner as the original.

c. Destroy intelligence materials in accordance with approved methods identified in the NISPOM.

d. Restrict access to those individuals with a valid need-to-know who are actually providing services under the contract. Further dissemination to other contractors, subcontractors, or other government agencies and private individuals or organization is prohibited unless authorized in writing by the Contracting Officer's Representative (COR) with prior approval of the Unit IN/SIO.

e. Not release intelligence data to foreign nationals or immigrant aliens, regardless of their security clearance or contract status, without advance written permission from the COR, Foreign Disclosure Policy Office and Unit IN/SIO.

f. Ensure that each employee having access to intelligence material is fully aware of the special security requirements for this material.

2. Returning Intelligence to the Air Force. Contractors must return intelligence data to the COR at the termination or completion of a contract unless the COR has provided written approval for the contractor to retain for an additional two years. If retention is required beyond the two year period, the contractor must again request and receive written retention authority from the COR. If the COR grants retention authority, the COR must provide a copy of the written approval to the Unit IN/SIO.

3. Release of Classified and Unclassified Intelligence Information to Foreign Government and Their Representatives. Any military activity or defense contractor receiving a request from a foreign government or a representative thereof, for intelligence data about this program, shall forward the request to the Unit IN/SIO for coordination with the cognizant foreign disclosure office. Information released under Foreign Military Sales (FMS) must comply with the specific USAF disclosure guidance issued for the specific FMS customer.

ATTACHMENT 3

DD Form 254 Block 10j - FOUO

1. FOR OFFICIAL USE ONLY INFORMATION:

- a. The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation by a DoD User Agency. It is not authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).
- b. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

2. IDENTIFICATION MARKINGS

- a. An unclassified document containing FOUO information will be marked "For Official Use Only" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion markings will be shown.
- b. Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, "FOUO."
- c. Any FOUO information released to a contractor by a DoD User Agency is required to be marked with the following statement prior to transfer:

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA Exemptions _____ apply.

- d. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. When the FOUO status is terminated, all known holders will be notified to the extent practical.

3. DISSEMINATION: Contractors may disseminate FOUO information to their employees and subcontractors who have a need for the information in connection with a classified contract. Dissemination will be accomplished in accordance with items 5 and 6 below.

4. STORAGE: During working hours, FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material; can be stored in locked receptacles such as file cabinets, desks, or bookcases.

5. TRANSMISSION: FOUO information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth class mail.

- a. Electronically Transmitted Messages: Electronic transmission of FOUO information should be by approved secure communication systems (STU-III, STE, secure fax, SIPRNet, etc.) whenever practical. When faxing, the recipient should be present to receive the FOUO material. Do not send FOUO information across the internet without an appropriate level of protection to prevent unintentional or unauthorized disclosure. Assume our adversaries will intercept everything sent on the internet. Some techniques for protecting FOUO going over the internet include: Utilization of the SIPRNet if this

capability exists within your organization, 3DES encryption utility or use a (Win) Zip file format to condense files and password-protect the zip file(s). When you password-protect a file you must then call that person or have them call you to tell them the password. Do NOT email the password.

6. DISPOSITION & DISCLOSURE: When no longer needed, FOUO information must be shredded by a cross-cut shredder. Unauthorized disclosure of FOUO information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

7. Unauthorized Disclosure: The unauthorized disclosure of UCI/FOUO material is not an unauthorized disclosure of classified information. However, Air Force and DoD contractor personnel have a duty to take reasonable actions to protect UCI/FOUO material under their control from unauthorized disclosure. Appropriate administrative action should be taken to prevent such disclosures.

ATTACHMENT 4

Reference Item 11i.

EMISSION Security (EMSEC) Requirements

1. The contractor shall ensure that compromising emanations conditions related to this contract are minimized. The following procedures relate to classified processing conducted within the US. Within NATO countries, prime contractors and sub-contractors using contractor or NATO-controlled equipment will adhere to NATO requirements for Emission Security (EMSEC) procedures. Contractors operating US-only equipment, whether in a NATO-controlled facility or US-controlled facility, must comply with Air Force EMSEC procedures as specified by the cognizant EMSEC Manager.
2. For contracts which require the processing of classified information in a contractor facility, the contractor shall provide countermeasure assessment data to the Contracting Officer (CO), in the form of an EMSEC countermeasures assessment Request (ESAR). The ESAR shall provide only specific responses to the data required in paragraphs 4.1 - 4.4, below. The contractor's standard security plan is unacceptable as a "stand-alone" ESAR response. The ESAR information will be used to complete an EMSEC assessment and countermeasures review of the contractor's facility, to be performed by the government EMSEC authority using current Air Force EMSEC directives.
3. The contractor will not process classified information until an ESAR is contractually submitted, the EMSEC assessment and countermeasures review have been conducted, and the system has been accredited/approved by the Cognizant Security Agency (CSA) in accordance with Chapter 8 of the NISPOM.
 - 3.1 Recognizing that contractors utilize Information Systems (IS) for multiple contracts, ESAR assessments compiled and approved for a particular system under one ESC contract are considered approved under other existing, follow-on and new ESC contracts for that particular contractor, as long as no changes are made to the security profile of the IS. The approval(s) should be kept on file for all affected contracts.
 - 3.2 Any requests for interim approval to process classified information, until ESAR information can be submitted and EMSEC procedures completed, must be approved by the CSA. Such interim approval should not exceed 90 days.
4. When any of the information required in paragraphs 4.1 – 4.4 below changes (such as equipment, location or classification level), the contractor shall notify the contracting officer of the changes so an EMSEC Reassessment may be accomplished. The contractor shall submit to the System Program Office (SPO) or contracting officer a new ESAR, specifically identifying the configuration changes. It should be submitted at least thirty (30) days before the changes are projected to occur. The provisions of Paragraph 3 apply to these changes.

4.1. SYSTEM DESCRIPTION

4.1.1 SYSTEM/FACILITY: Full name and address of company submitting request and RFP/contract number and duration. Also provide a brief title identifying the overall system or facility (e.g. XYZ Missile word processing system, ABC aircraft interactive graphics system, etc.).

4.1.2 LOCATION: Provide the following information for the facility where processing will take place.

4.1.2.1. Identify the address (including city, state, zip code, facility, building and room number) where the system or facility is located. If the address is the same as 4.1.1., only indicate the building and room number where the equipment is located.

4.1.2.2. Make, title, and attach drawings/maps showing the inspectable space (See 4.1.2.2.1), Controlled Access Areas (See 4.1.2.2.2), and floor layout of the RED and BLACK equipment. The floor layout of the equipment (RED and BLACK) should include the locations of any transmitters, transceivers, and cryptographic equipment, as well as RED and BLACK IS. The drawing may be free hand. Include the scale (roughly). Indicate on the map surrounding buildings to a distance of 200 meters. Identify significant occupants, organizations, and activities in the buildings within 200 meters. If the U.S. Government or the contractor identified in 4.1.1 above does not wholly occupy the building containing the RED equipment, identify and indicate the location of those other occupants.

4.1.2.2.1. **Definition of Inspectable Space**—The three-dimensional space surrounding equipment that processes classified or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify or remove a potential TEMPEST exploitation exists.

4.1.2.2.2. **Definition of Controlled Access Area (CAA)**—The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and

are either escorted by authorized persons or are under continuous physical or electronic surveillance.

4.2. RESPONSIBLE PERSONNEL:

4.2.1 INFORMATION SYSTEM SECURITY MANAGER (ISSM): Provide name, title, office symbol and telephone number. Include the same for the Company Appointed EMSEC (TEMPEST) Authority, if applicable.

4.2.2 SYSTEM CUSTODIAN: If different from above, provide name, title, and office symbol and telephone number.

4.3. OPERATIONAL RISK:

4.3.1 Identify the highest level of classified processing.

4.3.2 Provide an estimate of the total classified processing volume in a given measure of time. The estimate can be in hours per day, pages of classified generated per week, or megabytes or gigabytes processed per day/month. (e.g., 2 hrs/day, 15 pages/mo, or 320 mb/week) , AND a percentage of total material processed for each level (e.g. 10% Top Secret; 55% Secret; 20% Confidential; 15% unclassified).

4.4 EQUIPMENT:

4.4.1 List the manufacturer and exact model number, nomenclature (terminal, disk drive, video system, etc.) and quantity of each equipment involved in classified processing. Do not provide a complete inventory of all the company's processing equipment.

4.4.2 List any encryption equipment (i.e., STU-III, KG-84, KG-194, etc.), that might be used for processing and transmission of classified information.

4.4.3. List any transmitters/transceivers (SATCOM, RF, UHF/VHF, WLAN, etc.) operating in the area (same room and adjacent rooms) of the equipment processing classified information, and indicate their approximate distance from the RED equipment.

5.0 EMSEC is applied on a case-by-case basis and further information may be required to complete the ESAR; should this be the case, the contractor shall provide this information to the contracting officer, PMO or SPO when requested.

6.0 Current requirements of AFI 33-214 Vol. 2 and AFI 33-203 dictate that the information used to complete the EMSEC Assessment and Countermeasures Review be validated annually. The ISSM shall certify annually to the PMO, SPO, or contracting officer that no changes to the information provided in paragraphs 4.1 through 4.4 of the ESAR have occurred.

7.0 The prime contractor shall ensure that this EMSEC requirement is provided to all subcontractors and/or vendors. The subcontractors and/or vendors shall comply with these EMSEC requirements when classified processing related to this contract is necessary. Subcontractors and/or vendors will provide their ESAR through the prime contractor to the government contracting officer.

8.0 WITH THE EXCEPTION OF 3.2 ABOVE, CLASSIFIED PROCESSING WILL NOT BE DONE UNTIL THE ABOVE PROCEDURES ARE COMPLIED WITH AND THE IS HAS BEEN ACREDITED BY THE COGNIZANT SECURITY AGENCY (CSA).

9.0 If you have any questions feel free to contact Mr. Alfred Knoll, Hanscom AFB EMSEC Manager.

Mailing Address: ESC/NI6O
50 Hamilton Street
Hanscom AFB, MA
01731-1621

E-Mail: Alfred.Knoll@hanscom.af.mil
SIPRNet: Alfred.knoll@hanscom.af.smil.mil
Phone: (781) 377-4716
Fax Number: (781) 377-0562
STU-III Number: (781) 377-3497

ATTACHMENT 5

DD Form 254, Block 11j - OPSEC

The contractor will accomplish the following minimum requirements in support of the User Agency Operations Security (OPSEC) Program. Document items of critical information applicable to operations. Items of critical information are those facts, which individually, or in the aggregate, reveal sensitive details about the contractor's security operations, and thus require protection from adversarial collection or exploitation.

OPSEC Program managers will provide Airborne, Maritime/ Fixed Station (AMF) JTRS critical information (CI) lists to the contractor under separate cover. Contractors will participate in the installation OPSEC Program. Contractors will receive periodic training along with military and Government civilian counterparts.

The contractor will comply with the Department of Defense Web Site Administration Policies & Procedures dated 25 Nov 98 (with amendment April 26, 2001) developed by the Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence). This policy applies to all information being posted to web sites both publicly and non-publicly accessible.